Kerby Guillaume

The NICE Framework was developed to establish organized structure within the cybersecurity workplace. These help associates within the organization with their operation tasks in order to produce overall efficiency. The framework is broken down to different categories which emphasize certain points of interest regarding cybersecurity. One of these categories are the specific work roles of the associates. The roles include communication security management, cybersecurity planning, workforce management, curriculum development, instruction, legal advice, leadership, privacy compliance, product support management, program management, control assessment, system authorization, systems security management, technology portfolio management, and lastly, program auditing. According to the provided article, the work roles are designed to **“provide leadership, management, direction, and advocacy so the organization may effectively manage cybersecurity-related risks to the enterprise and conduct cybersecurity work”**.

As we can see there are various roles that are important to cybersecurity workplaces and those who work in cybersecurity have many tasks at hand. However, I do favor some tasks more than others as I see them to be more necessary for an organization. My top three roles are systems security management, privacy compliance, and technology program auditing.

**Systems Security Management.** System Security Management is at the top of my list due to the fact that it prioritizes cybersecurity risk management as a whole. Security and protection must always be the initial priority and in this role, associates must work to ensure protection against cyber crime, unauthorized access, and other malicious acts that could potentially lead to cyber attacks.

**Privacy Compliance.** In accordance with the duties of system security management, privacy compliance also focuses on the protection within cybersecurity. Although this also works towards the prevention of cyber attacks, privacy focuses more on the ethics of information used within the organization. Those who work in this role ensure that an organization’s data practices align with legal and ethical standards while protecting sensitive information from unauthorized access. In doing so, trust is built within the organization and its customers which is key to fulfilling a great business.

**Technology Program Auditing.** This role focuses primarily on the handling of information about the business. Associates work towards ensuring quality to provide the best services to their customers. These audits work in order to improve the flow of business by assuring that all functions work to satisfy the needs of customers and they also protect the business with risk management procedures.

My lowest ranked category would be cybersecurity curriculum development. Now this role focuses on developing certain forms of training and it can be important. However, while this can help associates, I don’t believe education should be a specific role as it doesn’t necessarily benefit the company as a whole.